REMARKS/ARGUMENTS

Background Information

Basically a feature of the present disclosure is to enable a software purchaser, who has purchased the software code from a reseller, to check that the purchased code is authentic (that is, it has not been modified). The purchaser wants to be assured that they got the real thing. Although the software purchaser only need communicate with the software reseller, the authenticity of the code is verified by the software owner by having the software reseller contact the software owner.

To ensure that the reseller sends the purchased code to the software owner (rather than a different version), the purchased code is used as the encryption key string in an IBE (Identifier Based Encryption) encryption of an arbitrary item of data (the 'first data' of claim 1) supplied by the purchaser. The encryption key string is passed by the reseller to the software owner who checks that it represents the unmodified code; if this check is passed, the encryption key string is used to generate a decryption key for enabling the reseller to decrypt the encrypted first data. After decrypting the first data with the decryption key, the reseller returns the decrypted first data to the purchaser thereby reassuring the purchaser that the purchased code is authentic. If the reseller modifies the encryption key string before passing it to the software owner (for example, because the reseller modified the code before selling it and knows that the authentic code must be passed to the software owner), the decryption key (for the unmodified code) will not correctly decrypt the first data and the software owner is not going to verify the modified code by returning a decryption key associated with it. So the software purchaser is alerted that something is amiss when the reseller cannot decrypt the encrypted first data.

One clarification being made to claim 1 by this response. To ensure that it is clear that the encryption being talked about in the second sub-paragraph of the claim is the same encryption as mentioned in the first sub-paragraph, the second sub-paragraph has been amended as follows:

"the encryption of the first data by the user entity is effected using, as encryption parameters, both an encryption key string comprising said software code or a representation thereof, and public data of said party".

With respect to the rejection under 35 USC 112, the word "if" has been amended to "provided". If the Examiner objects to the "the or each validation check" phraseology, that phraseology is perfectly consonant with the use of "at least one validation check" earlier in the claim.

Regarding the 35 USC 102 Rejection, the Kramer reference (US 6,986,040) is not even close. Kramer appears to be a standard key distribution scheme applied to a particular environment. The abstract gives a reasonable overview of the disclosure of Kramer: a ticket service generates session keys and when a client wishes to communicate with an application, one copy of a session key is passed over a secure link to the client together with an identifier. The client passes the identifier to the application which uses it to retrieve its own copy of the same session key from the ticket service (or its agent).

It is very difficult to see how the examiner can equate the disclosure of Kramer to the present claims. The main passage of Kramer relied upon by the Examiner is col. 6, lines 29 – 48 (see page 3 of the Official Action).

In particular, lines 29-33 are asserting as anticipating the second sub-paragraph of claim 1; this sub-paragraph is about encrypting the first data "using, as encryption parameters, both an encryption key string comprising said software code or a representation thereof, and public data of said party". Lines 29-33, col. 6 of Kramer is about the client sending a session ID to the

application server either in encrypted or cleartext form. The examiner therefore appears to be equating the 'first data' of claim 1 with the session ID of Kramer. But nothing is said in Kramer about how the session ID is encrypted by the client[1] – what is clear is that the session key cannot be used for this purpose since the application server does not yet possess the session key and can only obtain it by decrypting the encrypted session ID (which it obviously cannot do if the session key has been used to encrypt the session ID). Absent any details of how the session ID might be encrypted by the client, it is impossible to assert that the referenced passage of Kramer discloses the claim 1 feature of:

"using, as encryption parameters, both an encryption key string comprising said software code or a representation thereof, and public data of said party"

The third sub-paragraph of claim 1 concerns the provision of the decryption key by the 'party' to the software provider only if the software code provided to the user entity is valid. The referenced passage of Kramer (col. 6, lines 33-48) is about how the application server uses the session ID to obtain the session key which the application server then uses for secure communication between itself and the client. At best, it might be said that obtaining the decryption key in claim 1 is similar to obtaining the session key in Kramer – however, this would equate the decryption key of claim 1 with the session key of Kramer and the software code of claim 1 to the session ID (because in Kramer the validity of the session ID is checked before the session key is released whereas in claim 1 it is the validity of the software code that is checked before the decryption key is released). Of course, such a mapping of the features of Kramer to the features of claim 1, merely shows the invalidity of the examiner's arguments; not only has the session ID already been equated to the first data

[1] It is known in the art how to encrypt the session key - but that is not what is be referred to here - this art does not teach encrypting the session ID.

(see previous paragraph) so equating it also to the software code does not seem logical. Moreover, it is difficult to see how the session ID of Kramer can be considered 'software code'. Furthermore, no details are given in Kramer about generation of the session key so it would not seem possible for Kramer to satisfy the requirement of the third sub-paragraph of claim 1:

"generation of this key (the decryption key) by the party using both private data related to said public data, and the encryption key string or a corresponding reference string based on a reference version of the software code."

Additionally the session key of Kramer is a symmetric key whereas claim 1 uses an asymmetric key pair with the decryption key being generated from the encryption key. And as has been stated, Kramer does not suggest software code (or a 'representation of software code') as being used to form an encryption key. These differences serve to patentably distinguish all of the claims pending in this application over Kramer.

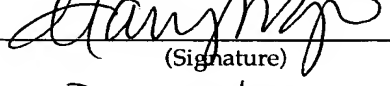
Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

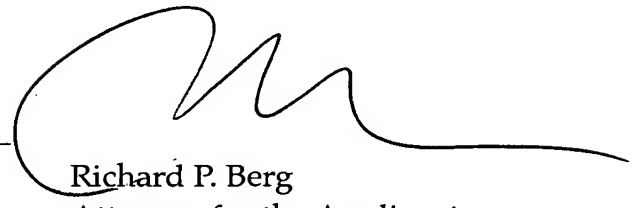
13 December 2006
(Date of Deposit)

Mary Ngo
(Name of Person Depositing)


(Signature)

13 December 2006
(Date)

Respectfully submitted,



Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile